CLAIMS

What is claimed is:

1. A method for securely transferring data across an optical-switched (OS) network, comprising:

distributing security keys to edge nodes in the OS network;

encrypting, at a source edge node, data to be sent from the source edge node to a destination edge node, said data encrypted with a security key distributed to the source node;

sending the data along a virtual lightpath between the source and destination edge nodes, the virtual lightpath spanning at least one lightpath segment; and

decrypting, at the destination edge node, the encrypted data that are sent.

2. The method of claim 1, wherein the OS network comprises an optical burst-switched (OBS) network.

3. The method of claim 2, wherein the OBS network comprises a photonic burst-switched (PBS) network.

4. The method of claim 2, wherein the PBS network comprises a wavelength-division multiplexed (WDM) PBS network.

5. The method of claim 1, wherein the security keys are distributed by distributing a common decryption and encryption key pair to each of the edge nodes.

6. The method of claim 1, wherein the security keys are distributed by:

distributing a respective decryption key to each of the edge nodes, each respective decryption key being particular to its node; and

distributing respective sets of encryption keys to each node, each set of encryption keys for a given node including encryption keys corresponding to the decryption keys distributed to each of the other edge nodes.

7. The method of claim 1, wherein the security keys are distributed by:

distributing a respective private key to each of the edge nodes, each respective private key being particular to its node; and

distributing respective sets of digital certificates sets to each node, each set of digital certificates for a given node containing a set of public keys corresponding to the private keys distributed to each of the other edge nodes.

8. The method of claim 6, further comprising self-generating the digital certificates.

9. The method of claim 8, further comprising:

for each edge node,

self-generating an digital certificate containing a public key that is asymmetric to the private key for the edge node; and

sending the digital certificate to each of the other edge nodes.

10. The method of claim 9, further comprising:

for at least one node,

generating a private key for the edge node via key-generation facilities provided by the edge node; and

generating the public key for the edge node via the key-generation facilities.

11. The method of claim 7, further comprising:

sending security data to a certificate authority, the security data defining public keys that are to be included in respective digital certificates; and

receiving authenticated digital certificates from the certificate authority.

12. The method of claim 11, wherein the security data is sent from an administrator of the OBS network.

13. The method of claim 9, further comprising:

generating a respective set of security data at each edge node; and

sending the respective set of security data from each edge node to the certificate authority.

14. The method of claim 1, further comprising sending security keys to the edge nodes using a communication channel that is external to the OBS network to distribute the security keys.

15. The method of claim 1, further comprising sending security keys to the edge nodes using an out-of-band channel of the OBS network to distribute the security keys.

16. The method of claim 15, further comprising sending security data via a control burst for the OBS network, the security data including one or more security keys or containing information from which one or more security keys can be derived.

17. The method of claim 1, further comprising sending information to each edge node identifying at least one of an encryption algorithm and decryption algorithm to be employed to encrypt and/or decrypt the data via the security keys.

18. The method of claim 17, further comprising sending encryption and/or decryption code to an edge node, the encryption and/or decryption code to be executed to perform encryption and/or decryption operations.

19. A machine-readable medium to provide instructions, which when executed by a processor in a source edge node of an optical switched (OS) network cause the source edge node to perform operations including:

encrypting data to be sent to a destination edge node;

generating a control burst, the control burst containing information to reserve network resources to form a virtual lightpath between the source edge node and the destination edge node during a scheduled timeslot, the virtual lightpath including at least one lightpath segment;

embedding information in the control burst identifying one or more data bursts to be sent from the edge node to the destination edge node will be encrypted;

sending the control burst to a first hop along the virtual lightpath, the first hop comprising one of a switching node or the destination edge node; and

sending said one or more data bursts containing the data that are encrypted to the first hop along the virtual lightpath during the scheduled timeslot.

20. The machine-readable medium of claim 19, wherein execution of the instructions further perform the operation of sending an encryption key to each of a plurality of edge nodes in the OS network.

21. The machine-readable medium of claim 20, wherein execution of the instructions performs the operation of sending the encryption key to an edge node by:

generating a control burst containing security data including the encryption key or data from which the encryption key can be derived; and

sending the control burst to a first hop along a virtual lightpath coupling the edge node sending the control burst to and edge node receiving the control burst, the first hop comprising one of the edge node receiving the control burst or a switching node.

22. The machine-readable medium of claim 21, wherein the security data include an digital certificate.

23. The machine-readable medium of claim 22, wherein execution of the instructions performs the further operation of generating a self-signed digital certificate.

24. The machine-readable medium of claim 21, wherein the security data include one of information identifying an encryption algorithm used to encrypt the data or executable code that may be used to decrypt the certificate.

25. The machine-readable medium of claim 20, wherein an encryption key is sent to an edge node via a communication channel that is external from the OS network.

26. The machine-readable medium of claim 19, wherein execution of the instructions performs further operations including:

generating an encryption key, the encryption key to be used to encrypt the data; and

generating a decryption key corresponding to the encryption key.

27. The machine-readable medium of claim 19, wherein execution of the instructions performs further operations including:

generating security data including the decryption key and identifying the decryption key as a public key, the security data comprising data from which an digital certificate may be issued; and

sending the security data to a certificate authority.

28. A system comprising:

at least one processor;

memory coupled to said at least one processor;

an encryption component;

an optical interface; and

a storage device in which instructions are stored, said instructions to perform operations when executed by said at least one processor, including:

invoking the encryption component to encrypt data to be sent to a destination edge node operatively linked in communication to the system via a photonic burst-switched (PBS) network, the system to operate as a source edge node;

generating a control burst, the control burst containing information to reserve PBS network resources to form a virtual lightpath between the source edge node and the destination edge node during a scheduled timeslot, the virtual lightpath including at least one lightpath segment;

embedding information in the control burst identifying one or more data bursts to be sent from the source edge node to the destination edge node will be encrypted;

sending the control burst to a first hop along the virtual lightpath, the first hop comprising one of a switching node or the destination edge node; and

sending said one or more data bursts containing the data that are encrypted to the first hop along the virtual lightpath during the scheduled timeslot.

29. The system of claim 28, wherein said at least one processor includes a network processor.

30. The system of claim 29, wherein said at least one processor includes an ingress network processor and an egress network processor.

31. The system of claim 30, wherein the encryption component comprises a hardware device programmed to perform encryption operations.

32. The system of claim 30, wherein the encryption component is embodied as a software module comprising a plurality of instructions to effectuate encryption operations when executed on a processor.

33. The system of claim 28, further comprising a decryption component configured to decrypt data received from the PBS network.

34. The system of claim 33, wherein the decryption component comprises a hardware device programmed to perform decryption operations.

35. The system of claim 33, wherein the decryption component is embodied as a software module comprising a plurality of instructions to effectuate decryption operations when executed on a processor.

36. The system of claim 28, further comprising a key generation component.

37. The system of claim 36, wherein the key generation component comprises a hardware device programmed to generate security keys.

38. The system of claim 36, wherein the key generation component is embodied as a software module comprising a plurality of instructions to effectuate generation of security keys.